UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/654,347	08/30/2000	Douglas B. Moran	RECOP017	5971

21912 7590 07/06/2005

VAN PELT, YI & JAMES LLP
10050 N. FOOTHILL BLVD #200
CUPERTINO, CA 95014

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/654,347	MORAN, DOUGLAS B.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 May 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12,16 and 17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12,16 and 17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *5/2/05*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 02 May 2005.

2. Claims 1-12,16,17 are pending for examination.

3. Claims 1-12,16,17 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 3 recites the limitation " level in ***the directory*** " in claim 3. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-12,16,17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Porras et al, U.S. Patent 6,704,874 B1, and further in view of Beardsley et al, U.S. Patent 5,471,631.

4. As per claim 1; "A system for detecting intrusions on a host [Porras et al, col. 1,lines 20-31, col. 2,lines 19-38, col. 3,lines 46-62, col. 12,lines 8-59], comprising:

a sensor for collecting information including events and timestamps from a logfile [Porras et al, col. 1,lines 34-62, col. 52-65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 10,lines 39-45, col. 13,lines 15-23]; and

an analysis engine configured to

identify a backward time step in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a second log entry log entry time associated with a second log entry entered in the log prior to the first entry, [Porras et al, col. 3,lines 30-40, col. 6,lines 13-col. 7,line 8, col. 12,lines 45-58, whereas the general timestamp/temporal nature of event log timestamps processing is taught per se.],

correlate the backward time step with an event, and

assign a suspicion value to the event [Porras et al, col. 1,lines 34-col. 2,line 65, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6]."

6. Claim 2 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is configured to identify a time step as forward if a timestamp of an entry in the logfile is later than an preceding entry in the logfile, and identify a time step as backward if a timestamp of an entry in the logfile is earlier than an preceding entry in the logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 13,lines 15-23) suggest such limitations.

7. Claim 3 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is further configured to use expected activity level in the directory to determine the suspicion value.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 3,lines 30-40,54-62, col. 6,lines 1-57, col. 8,lines 37-col. 9,line 6, col. 10,lines 39-45, col. 12,lines 8-col. 13,line 23) suggest such limitations.

8. Claim 4 ***additionally recites*** the limitations that; "The system as recited in claim 1, further comprising a second sensor for collecting information including events and timestamps from a second logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 5,lines 63-col. 6,line 13, col. 7,lines 55-66) suggest such limitations.

9. Claim 5 ***additionally recites*** the limitations that; "The system as recited in claim 4, wherein the analysis engine is configured to correlate a time step in the logfile with an event in the second logfile.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 5,lines 63-col. 6,line 13, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6) suggest such limitations.

10. Claim 6 ***additionally recites*** the limitations that; "The system as recited in claim 1, wherein the analysis engine is further configured to filter out expected time steps from further analysis.". The teachings of Porras et al (col. 1,lines 34-col. 2,line 65, col. 6,line 58-col. 7,line 8, col. 8,lines 37-col. 9,line 6) suggest such limitations.

11. Claim 7 ***additionally recites*** the limitations that; "The system as recited in claim 6, wherein the analysis engine is configured to filter out expected backward time steps by correlating them to Network Time Protocol adjustments.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57) suggest such limitations.

12. Claim 8 ***additionally recites*** the limitations that; "The system as recited in claim 6, wherein the analysis engine is further configured to compute an expected time drift resulting from a Network Time Protocol adjustment, and compare a forward time step in the logfile with the expected time drift.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57) suggest such limitations.

13. Claim 9 ***additionally recites*** the limitations that; "The system as recited in claim 8, wherein the analysis engine is further configured to compute a standard deviation of the expected time drift.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57, col. 8,lines 37-67) suggest such limitations.

14. Claim 10 ***additionally recites*** the limitations that; "The system as recited in claim 9, wherein the analysis engine is further configured to label time steps with weighted distributions.". The teachings of Porras et al (col. 3,lines 30-40, col. 6,lines 38-57, col. 8,lines 37-67) suggest such limitations.

15. Claim 11 ***additionally recites*** the limitations that; "The system as recited in claim 1, further comprising a user interface, and wherein the analysis engine is configured, upon correlating a time step to a record of an event in a logfile, to present the record to a user for labeling as to suspicion value.". The teachings of Porras et al (col. 7,lines 19-32, col. 9,lines 13-20) suggest such limitations.

16. Claim 12 ***additionally recites*** the limitations that; "The system as recited in claim 11, wherein the analysis engine is further configured to propagate the suspicion value to related events. The teachings of Porras et al (col. 6,lines 27-32, col. 7,lines 19-32,56-67, col. 9,lines 13-20, col. 10,lines 65-67) suggest such limitations.

17. As per claim 16, this claim is the method claim for limitations from the apparatus claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection.

And further as per claim 17, this claim is an embodied software claim for limitations from the method claim 16 above, and is rejected for the same reasons provided for the claim 16 rejection.

The teachings of Porras et al suggest the base claims limitations (see "As per claim 1, ... 16, ...17, ... Claim 2, ...3, ...4, ...11, ...12 ***additionally recites*** the limitations ..." paragraphs above) *without explicitly teaching* of "... identify a backward time step in the logfile by identifying a first entry for which an associated first log entry time is earlier in time than a

second log entry log entry time associated with a second log entry entered in the log prior to the first entry ..." for the event log timestamps processing.

Beardsley et al, teaches of using time stamps to correlate data processing event times in connected data processing units (i.e., relative skewed clock or time tagged log entry correction upon found discrepancies in said time tags; Beardsley et al figures 1-8 and associated descriptions). The Beardsley et al invention also clearly encompasses the logging of detected intrusions on a host aspects on a host system.

Thus, it would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to combine the Porras et al system for detecting/logging/analysis thereof, and intrusions on a host, with the Beardsley et al teachings of using time stamps to correlate data processing event times in connected data processing units in order to provide the detecting/logging/analysis system with a more robust log analysis capability.

Such motivation to combine would clearly encompass the need to allow "solving and recovering from error conditions ... in identification of reasons for peripheral subsystem and data processing system failures [i.e., intrusion detection per se, and the results thereof]. ...it is critical that data processing events, ... preceding a data processing failure event be quickly and easily identified. Such identification has been difficult because there is no time correlation of error logs kept in a subsystem and error logs kept in a host processor relating to such data processing events. ..." (i.e., Beardsley et al col. 1,lines 36-53).

Conclusion

18. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100